Standard Operating Procedure RTTC SYSRULES Policies and Procedures

1.0 INTRODUCTION

The process of requesting and receiving a user account from the RTTC Distributed Center implies acceptance of the rules and regulations of the RTTC Distributed Center.

2.0 GENERAL REGULATIONS

1. In order to access the system a user must be issued a passcard, have chosen or been issued a pin number and a Kerberos password. The user will take all reasonable steps to insure that any passwords and pin numbers assigned are properly safeguarded. At no time may a password be revealed to another individual. The passcode card should be in the possession of the responsible individual. If this is not possible, the user must employ reasonable measures to safeguard the card and prevent it from being stolen or used by other persons.

2. Should a card be lost or stolen, the user shall report the loss immediately to the RTTC Distributed Center Director, S/AAA@rttc.redstone.army.mil or (256)876-5669.

3. If the user has reason to suspect that his account or password has been compromised in any way, the user shall report this immediately to the RTTC Distributed Center Director who will initiate corrective action.

4. Access rules are clear and straight forward. At the time a user is given access to the system, his

working filesystem and disk allotment will be determined and communicated. At no time may the user attempt to access space in areas not assigned to the user. User processes should not deliberately use scratch space in system temp directories. Users should not attempt to access information, data or programs in disk space assigned to other users. Regardless of the privileges assigned to user files, the assumption is made that all user data is private. Access (sharing of code or data) to files of another user must be by consent and with consideration for the sensitivity level of the information. User's who are discovered breaking this requirement will be disciplined, and may be terminated.

5. All users must read the Distributed Center's Automated Information Security Briefing before activation of their account and once a year thereafter. Users are bound by the regulations and understandings laid out by the AIS Security Briefing. A copy of this briefing will be sent by e-mail on request. It is also available here.

6. Users will Kerberos login to the RTTC DC system snoopy.redstone.army.mil. This machine is entirely interactive. RTTC does not provide batch queuing environments. Load balancing is provided by the RTTC DC staff. If there are any problems, please contact the RTTC DC system administration staff.

Click here for a printable version of this page.
Adobe Acrobat Reader is required.

Back to Top
Please read this Privacy & Security Notice
Last updated January 2, 2002
Please send questions or comments about this page to webmaster@rttc.army.mil